

"This document has not been reviewed by NASA Form 1676, NASA Document Availability Authorization (DAA), to determine to whom it may be disseminated or released; therefore, this information is considered Sensitive But Unclassified (SBU) and restricted to NASA Personnel Only until appropriate release approval has been determined by the DAA review. Contact the appropriate NASA Center to request a DAA review."

Number partitioning via quantum adiabatic computation

V. N. Smelyanskiy^{1,*} and U.V. Toussaint²

¹*NASA Ames research Center, MS 269-2, Moffet Field, Ca 94035-1000 and*

²*Max-Planck-Institute for Plasma Physics, Boltzmannstr. 2 D-85748 Garching*

(Dated: February 19, 2002)

We study both analytically and numerically the complexity of the adiabatic quantum evolution algorithm applied to random instances of combinatorial optimization problems. We use as an example the NP-complete set partition problem and obtain an asymptotic expression for the minimal gap separating the ground and excited states of a system during the execution of the algorithm. We show that for computationally hard problem instances the size of the minimal gap scales exponentially with the problem size. This result is in qualitative agreement with the direct numerical simulation of the algorithm for small instances of the set partition problem. We describe the statistical properties of the optimization problem that are responsible for the exponential behaviour of the algorithm.

PACS numbers: Valid PACS appear here

Since the discovery by Shor [1] nearly a decade ago of a quantum algorithm for efficient integer factorization there has been a rapidly growing interest in the development of new quantum algorithms capable of solving computational problems that are practically intractable on classical computers. Perhaps the most notable example of such problems is that of combinatorial optimization (COP). In the simplest case the task in COP is to minimize the cost function ("energy") $E_{\mathbf{z}}$ defined on a set of 2^n binary strings $\mathbf{z} = \{z_1, \dots, z_n\}$ $z_j = 0, 1$, each containing n bits. In quantum computation this cost function corresponds to a Hamiltonian H_P

$$H_P = \sum_{\mathbf{z}} E_{\mathbf{z}} |\mathbf{z}\rangle \langle \mathbf{z}| \quad (1)$$

$$|\mathbf{z}\rangle = |z_1\rangle_1 \otimes |z_2\rangle_2 \otimes \dots \otimes |z_n\rangle_n.$$

where the indices $z_j = 0, 1$ and the summation is over 2^n states $|\mathbf{z}\rangle$ forming the computational basis of a quantum computer with n qubits. State $|z_j\rangle_j$ of the j -th qubit is an eigenstate of the Pauli matrix $\hat{\sigma}_z$ with eigenvalue $S_j = 1 - 2z_j$ ($S_j = \pm 1$). It is clear from the above that the ground state of H_P encodes the solution to the COP with cost function $E_{\mathbf{z}}$.

COPs have a direct analogy in physics, related to finding ground states of classical spin glass models. In the example above bits z_j correspond to Ising spins S_j . The connection between the properties of frustrated disordered systems and the structure of the solution space of complex COPs has been noted first by Fu and Anderson [2]. It has been recognized [3] that many of the spin glass models are in almost one-to-one correspondence with a number of COPs from theoretical computer science that form a so-called NP-complete class [4]. This class contains hundreds of the most common computationally hard problems encountered in practice, such as constraint satisfaction, traveling salesmen, integer programming, and others. NP-complete problems are char-

acterized in the worst cases by exponential scaling of the running time or memory requirements with the problem size n . A special property of the class is that any NP-complete problem can be converted into any other NP-complete problem in polynomial time on a classical computer; therefore, it is sufficient to find a deterministic algorithm that can be guaranteed to solve all instances of just one of the NP-complete problems within a polynomial time bound. However it is widely believed that such an algorithm does not exist on a classical computer. Whether it exists on a quantum computer is one of the central open questions. Ultimately one can expect that the behavior of the new quantum algorithms for COPs and their complexity will be closely related to the properties of quantum spin glasses.

Farhi and co-workers suggested recently a new quantum algorithm for solving combinatorial optimization problems which is based on the properties of quantum adiabatic evolution [5]. Running of the algorithm for several NP-complete problems has been simulated on a classical computer using a large number of randomly generated problem instances that are believed to be computationally hard for classical algorithms [6–8]. Results of these numerical simulations for relatively small size of the problem instances ($n \leq 20$) suggest a *quadratic* scaling law of the run time of the quantum adiabatic algorithm with n . In [5, 9] special symmetric cases of COP were considered where symmetry of the problem allowed to describe the true asymptotic behavior ($n \rightarrow \infty$) of the algorithm. In certain examples considered in [9] quantum adiabatic algorithm finds the solution in time polynomial in n while simulated annealing requires exponential time. However, so far there are no analytical results on the asymptotic behavior of the algorithm for the general case of randomly generated hard instances of NP-complete problems.

In what follows we derive the asymptotic complexity of the quantum adiabatic algorithm for the Set Partition Problem (SPP). It is one of the six basic NP-complete problems that are at the heart of the theory of NP-completeness [4]. It can be formulated as com-

*Electronic address: vadim@email.arc.nasa.gov

binatorial optimization problem: Given a sequence of positive numbers $\{a_0, a_1, \dots, a_n\}$ find a partition, i.e. two disjoint subsets \mathcal{A}_1 and \mathcal{A}_2 such that the residue $E = \left| \sum_{a_j \in \mathcal{A}} - \sum_{a_j \in \mathcal{A}'} \right|$ is minimized. Due to the obvious symmetry of the problem it is always possible to fix the assignment of one of the numbers, say a_0 , to a subset \mathcal{A}_1 . In SPP we search for the bit strings $\mathbf{z} = \{z_1, \dots, z_n\}$ (or corresponding Ising spin configurations $\mathbf{S} = \{S_1, \dots, S_n\}$) that minimize the energy or cost function $E_{\mathbf{z}}$

$$E_{\mathbf{z}} = |\Omega_{\mathbf{S}}|, \quad \Omega_{\mathbf{S}} = a_0 + \sum_{j=1}^n a_j S_j, \quad S_j = 1 - 2z_j, \quad (2)$$

Here $S_j = 1$ ($z_j = 0$) if $a_j \in \mathcal{A}$ and $S_j = -1$ ($z_j = 1$) if $a_j \in \mathcal{A}'$. The minimum partition can also be viewed as a ground state of the Ising spin glass, $-\Omega_{\mathbf{S}}^2$, with the Mattis-like (global) antiferromagnetic coupling, $J_{ij} = -a_i a_j$.

SPP also has many practical applications including multiprocessor scheduling [10], cryptography [11], and others. The interest in SPP also stems from the remarkable failure of simulated annealing to find good solutions, as compared with the solutions found by deterministic heuristics [12]. The apparent reason for this failure is due to the existence of order 2^n local minima whose energies are of the order of $1/n$ [13] which undermines the usual strategy of exploring the space of configurations \mathbf{S} through single spin flips.

The computational complexity of random instances of SPP depends on the number of bits b needed to encode the numbers a_j . Numerical simulations show [14, 15] that for independent, identically distributed (i.i.d.) random b -bit numbers a_j , the solution time grows exponentially with n for $n < b$ and polynomially for $n > b$. The transition from the "hard" to computationally "easy" phases has features somewhat similar to phase transitions in physical systems [16]. Transitions of this kind were observed in various NP-complete problems [17] and can be analyzed in the framework of statistical mechanics. In what follows we concentrate on the computationally hard regime $n \ll b$.

We now consider the distribution of the partition energies $E_{\mathbf{z}}$. It was derived in [18] using statistical averaging over the assemble of instances of SPP with i.i.d. numbers a_j . Bearing in mind our eventual goal of deriving the complexity of the quantum algorithm for a given random instance of SPP we do not perform such an averaging. Instead we work with a given set of $\{a_j\}$ and introduce a coarse-grained "density of states"

$$\rho(E) = \left\langle \sum_{\mathbf{z}} \delta(E - E_{\mathbf{z}}) \right\rangle. \quad (3)$$

Here the sum is over 2^n bit-strings \mathbf{z} ; partition energy $E_{\mathbf{z}}$ is defined in (2) and $\langle \dots \rangle$ denotes averaging over the interval of the partition values $(E - \eta/2, E + \eta/2)$ with the window size chosen self-consistently, $\eta \gg 1/\rho(E)$. Using

(2) we can rewrite (3) in the form

$$\rho(E) = \frac{2^{n+1}}{\pi} \int_0^\infty ds f\left(\frac{\eta s}{2}\right) I(s) \cos(Es), \quad (4)$$

where $I(s) = \prod_{j=0}^n \cos(a_j s)$ and $f(x) = \sin(x)/x$ is a window function that imposes a cut-off in the integral (4) at $s \sim 2/\eta \ll \rho(E)$. For large n this integral can be evaluated using the steepest descent method. To find the saddle points we shall assume that the b -bit numbers a_j are distributed inside of the interval $(0, 1)$ and are the integer multiples of 2^{-b} , the smallest number that can be represented with available number of bits. We note that for large n the function $I(s)$ has sharp maxima (minima) with width $\sim n^{-1/2}$ at the points $s_k = k\pi 2^b$, $k = 0, 1, \dots$; $|I(s_k)| = 1$. The sum over these saddle-points was evaluated by Mertens [16] who analyzed the partition function in SPP. In our case only one saddle point at $s = 0$ contributes to the integral (4). Indeed, it will be seen below that the window size $2/\eta$ can be chosen to obey the conditions $1 \ll n^{1/2}/\eta \ll 2^n$. Therefore in the high-precision case ($b \gg n$) saddle-points s_k with $k > 0$ lie far outside the window and their contributions can be neglected [?]. On the other hand the window function $f(x)$ can be replaced by unity while computing the contribution from the saddle-point at $s = 0$. Finally we obtain for $E \ll n$

$$\rho(E) = \frac{2^{n+1} \Theta(E)}{\sqrt{2} \pi \sigma^2 n} \exp\left(-\frac{E^2}{2\sigma^2 n}\right) + \mathcal{O}(n^{-3/2})$$

$$\sigma^2 = \frac{1}{n} \sum_{j=1}^n a_j^2 + \mathcal{O}(n^{-1}), \quad E \ll n. \quad (5)$$

Here Θ denote a step function. $\Theta(x)=1$, for $x \geq 0$ and $\Theta(x)=0$ for $x < 0$. The coarse-grained state density in Eq.(5) depends on the set of $\{a_j\}$ through a single self-averaging quantity σ^2 (cf. [16]). For E that are not too large ($E \lesssim \sqrt{n}$) the average separation between the individual partition energies $E_{\min} \sim \sqrt{n} 2^{-n}$. This justifies the choice of the window η above that corresponds to coarse-graining over many individual level separations. For a typical set of numbers $\{a_j\}$ there are only two scales present in the distribution of partition energies, one is a "microscopic" scale given by E_{\min} and another is given by the mean partition energy $\langle E \rangle = \sigma(2n/\pi)^{1/2}$.

Using the same approach one can derive the distribution $\bar{\rho}(\Omega)$ of $\Omega_{\mathbf{S}}$. For $|\Omega_{\mathbf{S}}| \ll n$ it is Gaussian, $\bar{\rho}(\pm\Omega) = 1/2\rho(|\Omega|)$ and can be understood in terms of a random walk with coordinate Ω (cf. (2)). The walk begins at the origin, $\Omega = 0$, and makes n steps. At the j -th step Ω moves to the right or to the left by "distance" $2a_j$ if $S_j = 1$ or $S_j = -1$, respectively. In the asymptotic limit of large n the result (5) corresponds to equal probabilities of right and left moves and the distribution of step lengths coinciding with that in the set of numbers $\{2a_j\}$.

We now consider the "conditional" density of the partition energies $\rho_r(E'|E) = \rho_r(E', E)/\rho(E)$ where $\rho_r(E'|E)$

is a “joint” density defined as follows

$$\rho_r(E', E) = \sum_{\mathbf{z}} \rho_{r,\mathbf{z}}(E') \delta(E - E_{\mathbf{z}}) \quad (6)$$

$$\rho_{r,\mathbf{z}}(E') = \left\langle \sum_{\mathbf{z}'} \delta(E' - E_{\mathbf{z}'}) \Delta_{r,D(\mathbf{z}',\mathbf{z})} \right\rangle \quad (7)$$

Here $\Delta_{k,l}$ is a Kronecker delta. Function $D(\mathbf{z}, \mathbf{z}')$ above computes the number of bits that take different values in the bit-strings \mathbf{z} and \mathbf{z}' , it is a so-called Hamming distance between the strings

$$D(\mathbf{z}, \mathbf{z}') = \sum_{j=1}^n (1 - z_j) z'_j + (1 - z'_j) z_j. \quad (8)$$

Conditional density $\rho_{r,\mathbf{z}}(E')$ in (7) determines the distribution of energies $E_{\mathbf{z}'}$ for the strings \mathbf{z}' obtained from \mathbf{z} by flipping r bits. Similar to Eq. (3), $\langle \dots \rangle$ in (6),(7) denotes averaging over the small energy interval $(E - \eta/2, E + \eta/2)$ that, however, includes many individual partition levels. For $r = 1$ there are exactly n strings \mathbf{z}' on a Hamming distance $r = 1$ from the string \mathbf{z} . Partition energies corresponding to these strings equal $|\Omega_S - 2a_j S_j|$, $1 \leq j \leq n$ (cf. (2)). One can show that for $E_{\mathbf{z}} < 2$ the distribution of these energies is nearly uniform in the range $(0, 2 - E_{\mathbf{z}})$ due to the fact that spins S_j are nearly equally distributed between ± 1 values for configurations with $|\Omega_S| \ll n$. Similar arguments apply for the case $r = n - 1$. Using a coarse-graining window such that $n^{-1} \ll \eta \ll 1$ one can obtain in the range of energies $E', E_{\mathbf{z}} \lesssim 1$ the following result:

$$\begin{aligned} \rho_r(E' | E_{\mathbf{z}}) &\approx \rho_{r,\mathbf{z}}(E') = n/2 + \mathcal{O}(1) \\ r &= 1, n-1, \quad n \gg 1. \end{aligned} \quad (9)$$

For large $r, n - r \gg 1$ one can calculate the conditional densities (6) for a given set of $\{a_j\}$ by evaluation of the appropriate integrals with the steepest descent method, in a similar manner to the derivation of $\rho(E)$ in Eqs.(3)-(5). Here we will skip the derivation and only provide the result that we found to be in a very good agreement with the numerical simulations of SPP even for relatively small $n \sim 20 - 30$. State density functions in (6) are given each by a sum of Gaussians for $E, E' > 0$ and have a broad maximum at the origin. Near the maximum we have:

$$\begin{aligned} \rho_r(E' | E_{\mathbf{z}}) &\approx \rho_{r,\mathbf{z}}(E') \approx \frac{\zeta(r/n)}{\sigma \sqrt{\pi n/2}} \binom{n}{r} \\ \zeta(x) &= (4x(1-x))^{-1/2}, \quad r, n-r \gg 1. \end{aligned} \quad (10)$$

This result applies in a range $E', E_{\mathbf{z}} \ll [nc(r/n)]^{1/2}$. We note that conditional density (7) is uniform there and does not depend on E' and \mathbf{z} after the coarse-graining over the small interval η of energies $E_{\mathbf{z}'}$ in (10). Window size $\eta \gg \binom{n}{r}^{-1}$.

Eqs. (9),(10) suggest the structure of the low-lying partition configurations. Bit strings \mathbf{z}' that are on a Hamming distance r from a given string \mathbf{z} correspond to a subset of partition energies with *average* spacing $\sim \binom{n}{r}^{-1}$

which does not depend on \mathbf{z} in the range $E_{\mathbf{z}}, E_{\mathbf{z}'} \lesssim 1$ for all r . The greater the Hamming distance between the strings - the closer their partition energies can be to each other - and vice versa. This is a basic property of SPP that gives rise to an exponentially large number of local minima in the relatively narrow range of energies $\mathcal{O}(1)$. In a typical instance of random SPP correlations between the Hamming distances to a given string (e.g., the solution to SPP) and partition energies essentially vanishes.

In the quantum adiabatic algorithm [5] one specifies the time-dependent Hamiltonian $H(t) = \tilde{H}(t/T)$

$$\tilde{H}(\tau) = (1 - \tau) V + \tau H_P, \quad (11)$$

where $\tau = t/T$ is dimensionless “time”. This Hamiltonian guides the quantum evolution of the state vector $|\psi(t)\rangle$ according to the Schrödinger equation $i \partial |\psi(t)\rangle / \partial t = H(t) |\psi(t)\rangle$ from $t = 0$ to $t = T$, the *run time* of the algorithm. H_P is the “problem” Hamiltonian given in (1). V is a “driver” Hamiltonian, that is designed to cause the transitions between the eigenstates of H_P . In this algorithm one prepares the initial state of the system $\psi(0)$ to be a ground state of $\tilde{H}(0) = V$. In the simplest case

$$V = - \sum_{j=0}^{n-1} \sigma_x^j, \quad |\psi(0)\rangle = 2^{-n/2} \sum_{\mathbf{z}} |\mathbf{z}\rangle, \quad (12)$$

where σ_x^j is a Pauli matrix for j -th qubit. Consider instantaneous eigenstates $|\phi_\alpha(\tau)\rangle$ of $\tilde{H}(\tau)$ with energies $\lambda_\alpha(\tau)$ arranged in nondecreasing order at any value of $\tau \in (0, 1)$

$$\tilde{H}|\phi_\eta\rangle = \lambda_\eta|\phi_\mu\rangle, \quad \eta = 0, 1, \dots, 2^n - 1. \quad (13)$$

Provided the value of T is large enough and there is a finite gap for all $t \in (0, T)$ between the ground and excited state energies, $g(\tau) = \lambda_1(\tau) - \lambda_0(\tau) > 0$, quantum evolution is adiabatic and the state of the system $|\psi(t)\rangle$ stays close to an instantaneous ground state, $|\phi_0(t/T)\rangle$ (up to a phase factor). Because $H(T) = H_P$ the final state $|\psi(T)\rangle$ is close to the ground state $|\phi_0(\tau = 1)\rangle$ of the problem Hamiltonian. Therefore a measurement performed on the quantum computer at $t = T$ ($\tau = 1$) will find one of the solutions of COP nearly with certainty. In the Landau-Zener picture a quantum transition away from the adiabatic ground state occurs most likely in the vicinity of the point $\tau^* \in (0, 1)$ where the energy gap $g(\tau)$ reaches its minimum (avoided-crossing region). The probability of the transition, $1 - |\langle \psi(T) | \phi_0(\tau = 1) \rangle|^2$, is small provided that

$$T \gg \frac{|H_{01}^*|}{\Delta g_{\min}^2}, \quad g_{\min} = \min_{0 \leq \tau \leq 1} [\lambda_1(\tau) - \lambda_0(\tau)] \quad (14)$$

Here $|H_{01}^*| = |\langle \phi_1 | \tilde{H} | \phi_0 \rangle|_{\tau=\tau^*}$. Even in the cases that are more complex than the Landau-Zener “2-level” picture

of nonadiabatic transitions the analysis of minimum gap g_{\min} can provide an important test for the complexity of the quantum adiabatic algorithm. E.g., if one can show that for a random COP g_{\min} decreases exponentially fast with the problem size n while $|H_{01}^*|$ does not decrease with n that would be a strong indication for exponential complexity of the algorithm in such problem.

As suggested in [5] the quantum adiabatic algorithm can be recast within the conventional quantum computing paradigm using the technique introduced by Lloyd [19]. Continuous-time quantum evolution can be approximated by a time-ordered product of unitary operators, $e^{-i(1-\tau_k)V\delta} e^{-i\tau_k H_P \delta}$, corresponding to small time intervals $(t_k, t_k + \delta)$. Operator $e^{-i(1-\tau_k)V\delta}$ typically corresponds to a sequence of 1(2)-qubit gates (cf. (12)). Operator $e^{-i\tau_k H_P \delta}$ is diagonal in the computational basis $|\mathbf{z}\rangle$ and corresponds to phase rotations by angles $E_{\mathbf{z}}\Delta$. Since in the case $n \ll b$, the average separation between the neighboring values of $E_{\mathbf{z}}$ is $1/\rho(E) = \mathcal{O}(2^{-n})$, the quantum device would need to support a very high precision of physical parameters (like external fields, etc) to control small differences in phases, $\mathcal{O}(2^{-n})$. Since this precision scales with n exponentially it would strongly restrict the size of an instance of SPP that could be solved on such quantum computer (this technical restriction is generic for COPs that involve high-precision numbers). To avoid this restriction we define a new cost function that takes values on a scale which is *logarithmic* in $1/\rho(E)$. I.e., we chose the cost to be an oracle-type function $\mathcal{E}_{\mathbf{z}}$ that takes a set of $M+1$ integer values $\varepsilon_k = -M+k$, $0 \leq k \leq M$

$$\mathcal{E}_{\mathbf{z}} = -k + M, \text{ for } \omega_k \leq E_{\mathbf{z}} < \omega_{k+1}, \quad (15)$$

$$\omega_k = (2^k - 1)\omega_0, \quad k = 0, \dots, M. \quad (16)$$

We set $\mathcal{E}_{\mathbf{z}} = \varepsilon_M = 0$ for *all* states with $E_{\mathbf{z}} \geq \omega_M$ where ω_M is a control parameter chosen sufficiently large so that $M = \mathcal{O}(n)$. The space of 2^n states $|\mathbf{z}\rangle$ is divided into $M+1$ subspaces \mathcal{L}_k , each determined by Eqs. (15) and (16) for a given k

$$H_P = \sum_{k=0}^M \varepsilon_k \sum_{\mathbf{z} \in \mathcal{L}_k} |\mathbf{z}\rangle \langle \mathbf{z}|. \quad (17)$$

Note that subspace \mathcal{L}_0 contains the solution(s) to the SPP. Dimension d_0 of \mathcal{L}_0 is controlled by the value of ω_0 in (16) which is another control parameter of the algorithm. We set $\omega_0 = K/\rho(0)$ where the integer $K \approx d_0 \gg 1$ is independent of n and determines how many times in average one needs to repeat the quantum algorithm in order to obtain the solution to SPP with probability close to 1.

Operator H_P projects any state $|\psi\rangle$ onto the states with partition energies in the range $0 \leq E_{\mathbf{z}} < \omega_M$. We assume that $\omega_M \ll \langle E \rangle$ so that the density function (5) is nearly uniform in this range. Therefore the dimensions of the subspaces \mathcal{L}_k grow exponentially with k : $d_k = d_0 2^k$ for $k < M$. This simplification does not affect the complexity of a quantum algorithm that spends most of the

time in “annealing” the system to much smaller partition energies, $\omega_M \gg E_{\mathbf{z}} \sim E_{\min} = \mathcal{O}(n^{1/2} 2^{-n})$.

We now consider a stationary Schrödinger equation (13) and obtain the minimum gap g_{\min} (14) in the asymptotic limit $n \rightarrow \infty$. To proceed we need to introduce a new basis of states $|\mathbf{x}\rangle = |x_1\rangle_1 \otimes |x_2\rangle_2 \otimes \dots \otimes |x_n\rangle_n$ where state $|x_j\rangle_j$ is an eigenstate of the Pauli matrix $\hat{\sigma}_x$ for the j -th qubit with eigenvalue $1 - 2x_j = \pm 1$. Driver Hamiltonian V can be written in the following form

$$V = \sum_{m=0}^n V_m \mathcal{I}^m, \quad \mathcal{I}^m = \sum_{x_1 + \dots + x_n = m} |\mathbf{x}\rangle \langle \mathbf{x}|. \quad (18)$$

For a particular case given in Eq. (12) we have $V_m = 2m - n$. Matrix elements of \mathcal{I}^m in a basis of states $|\mathbf{z}\rangle$ depend only on the Hamming distance $D(\mathbf{z}, \mathbf{z}')$ between the strings \mathbf{z} and \mathbf{z}'

$$\mathcal{I}_{\mathbf{z}, \mathbf{z}'}^m = I_{D(\mathbf{z}, \mathbf{z}')}^m \quad (19)$$

$$I_r^m = 2^{-n} \sum_{q=0}^{n-r} \sum_{p=0}^r \binom{n-r}{q} \binom{r}{p} (-1)^p \Delta_{m, q+p} \quad (20)$$

We now rewrite Eq. (13) in the form

$$|\Psi\rangle = \frac{\tau}{\lambda - \alpha V} H_P |\Psi\rangle, \quad \alpha \equiv \alpha(\tau) = 1 - \tau. \quad (21)$$

(we temporarily drop the subscript μ indicating the number of a quantum state and the argument τ in Ψ and λ). From (15)-(21) we obtain the equation for the amplitudes $\Psi_{\mathbf{z}} = \langle \Psi | \mathbf{z} \rangle$ in terms of the coefficients I_r^m

$$\begin{aligned} \Xi_k \Psi_{\mathbf{z}} &= \frac{\tau \Phi 2^{-n}}{\lambda - \alpha V_0} + \tau \sum_{\mathbf{z}' \neq \mathbf{z}} \mathcal{J}_{D(\mathbf{z}, \mathbf{z}')} \Psi_{\mathbf{z}'} \mathcal{E}_{\mathbf{z}'}, \quad \mathbf{z} \in \mathcal{L}_k \\ \Xi_k &\equiv \Xi_k(\lambda) = 1 - \tau \mathcal{J}_0(\lambda) \varepsilon_k, \quad \Phi = \sum_{\mathbf{z}'} \mathcal{E}_{\mathbf{z}'} \Psi_{\mathbf{z}'}. \end{aligned} \quad (23)$$

$$\mathcal{J}_r \equiv \mathcal{J}_r(\lambda) = \sum_{m=1}^n \frac{I_r^m}{\lambda - \alpha V_m}, \quad 0 \leq r \leq n.$$

We now make a key observation that the (coarse-grained) distribution of matrix elements $\mathcal{J}_{D(\mathbf{z}, \mathbf{z}')}$ for a given \mathbf{z} is determined by $\mathcal{J}_r(\lambda)$ and conditional density $\rho_{r, \mathbf{z}'}(E)$ (6). We compute a cumulative quantity

$$\sum_{\substack{\mathbf{z} \neq \mathbf{z}' \\ \mathbf{z} \in \mathcal{L}_k}} \mathcal{J}_{D(\mathbf{z}, \mathbf{z}')}(\lambda) \approx F_k(\lambda) + f_{\mathbf{z}, k}(\lambda) \quad (25)$$

$$F_k(\lambda) = \frac{\mu s(\lambda)}{2^{M-k}}, \quad s(\lambda) = \int_0^n dr \zeta(r/n) \binom{n}{r} \mathcal{J}_r(\lambda) \quad (26)$$

where $\mu = \Omega_M / \sqrt{\pi n \sigma^2 / 2}$ and $f_{\mathbf{z}, k}(\lambda)$ is a small correction that will be described below. Function $s(\lambda)$ can be evaluated using the explicit form of $\mathcal{J}_r(\lambda)$ that decays rapidly with r . E.g., for $|\lambda - \alpha V_0| \ll 1$ one has

$$\mathcal{J}_r(\lambda) = \binom{n}{r}^{-1} \sum_{m=1}^{n-r} \frac{2^{-n} \binom{n}{m+r}}{m} - 2^{-n} (\ln r + \gamma). \quad (27)$$

(γ is an Euler's constant) and $s(\lambda) \approx -\ln 2/(2\alpha)$. According to (27), $\mathcal{J}_r \approx (n/2 - r)^{-1} \binom{n}{r}^{-1}$ for $n/2 - r \gg 1$, and the integrand in $s(\lambda)$ is a smooth function of r . This corresponds to the interesting fact that contributions to the sum in (25) from states \mathbf{z} with $D(\mathbf{z}, \mathbf{z}') = r \ll n$ are small ($\mathcal{O}((r/n)^{1/2})$). In fact, the dominant contribution is of "entropic" nature: it comes from the large number of states $\mathbf{z} \in \mathcal{L}_k$ corresponding to Hamming distances, $1 \ll r \lesssim n/2$, and contributing each a small weight \mathcal{J}_r . The energies of these states are distributed, for a given r , according to $\rho_{r, \mathbf{z}'}(E) \approx \bar{\rho}_r$, and this explains why $F_k(\lambda)$ does not depend on \mathbf{z}' (cf. (10)).

We note that the entropic term F_k scales down with k exponentially fast ($\propto 2^{k-M}$), proportionally to the size of the window $\omega_{k+1} - \omega_k$ of partition energies corresponding to $\mathbf{z} \in \mathcal{L}_k$ (cf. (16)). When this window becomes too narrow the contributions to the sum in (25) from the states \mathbf{z} with $r = D(\mathbf{z}, \mathbf{z}') \sim 1$ are no longer described by the density of states ρ_r , due to the discreteness of the partition energy spectrum $E_{\mathbf{z}}$. E.g., for a given \mathbf{z}' in this case there could be either one or none of the states $\mathbf{z} \in \mathcal{L}_k$ with $D(\mathbf{z}, \mathbf{z}') = 1$, depending on the choice of \mathbf{z}' . Contributions to the sum in (25) from these states strongly depend on \mathbf{z}' and are described by the term $f_{\mathbf{z}', k}$

$$f_{\mathbf{z}', k}(\lambda) \approx \mathcal{J}_1(\lambda) \Delta_{1, D(\mathbf{z}, \mathbf{z}')} + \mathcal{O}(n^{-3}), \quad \mathbf{z} \in \mathcal{L}_k. \quad (28)$$

Here the omitted higher-order terms correspond to $D(\mathbf{z}, \mathbf{z}') \geq 2$. We note that the first-order term in (28) becomes greater than the entropic term F_k (25) for $M - k \gtrsim \log_2(\mu n^2)$.

Based on the above properties of $\mathcal{J}_{D(\mathbf{z}, \mathbf{z}')}$ we look for the solution of Eq. (23) in the avoided-crossing region as a sum of two terms

$$\Psi_{\mathbf{z}} = \tilde{u}_{\mathbf{z}} + \bar{u}_{\mathbf{z}}, \quad \mathbf{z} \in \mathcal{L}_k, \quad 1 \leq k \leq M \quad (29)$$

Here \bar{u}_k and $\tilde{u}_{\mathbf{z}}$ are slowly- and fast-varying functions of \mathbf{z} , respectively, that satisfy the following equations:

$$\Xi_k \bar{u}_{\mathbf{z}} = 2^{-n} \tau [\Phi(\lambda - \alpha V_0)^{-1} + s(\lambda) \bar{\Phi}], \quad (30)$$

$$\Xi_k \tilde{u}_{\mathbf{z}} = \tau \sum_{\mathbf{z}' \notin \mathcal{L}_0} \mathcal{J}_{D(\mathbf{z}, \mathbf{z}')} \mathcal{E}_{\mathbf{z}'} \tilde{u}_{\mathbf{z}'} + \tau \varepsilon_0 \sum_{\mathbf{w} \in \mathcal{L}_0} \mathcal{J}_{D(\mathbf{z}, \mathbf{w})} \Psi_{\mathbf{w}}.$$

We note that the amplitudes $\Psi_{\mathbf{w}}$ here correspond to the ground state(s) $|\mathbf{w}\rangle$ of the final Hamiltonian, $H_P|\mathbf{w}\rangle = \varepsilon_0|\mathbf{w}\rangle$ and the decomposition (29) applies only to amplitudes with $\mathbf{z} \notin \mathcal{L}_0$. The above system of equations is closed by adding the equation for $\Psi_{\mathbf{w}}$ given by (23) with $\mathbf{z} = \mathbf{w}$ and (29) taken into account.

Eq. (30) for $\bar{u}_{\mathbf{z}}$ is coupled to the rest of equations via relation between the *cumulative* terms $\Phi = \bar{\Phi} + \tilde{\Phi} + \Phi_0$. Here $\bar{\Phi} = \sum_{\mathbf{z}} \mathcal{E}_{\mathbf{z}} \bar{u}_{\mathbf{z}}$ is a part of Φ (23) contributed by a slow-varying component and similarly, $\tilde{\Phi} = \sum_{\mathbf{z}} \mathcal{E}_{\mathbf{z}} \tilde{u}_{\mathbf{z}}$. We compute the cumulative term $\tilde{\Phi}$ using equations for $\tilde{u}_{\mathbf{z}}$ in (30) and also Eqs. (23)-(26)

$$\tilde{\Phi} = -\kappa(\tau \mu s(\lambda)) \Phi_0, \quad \Phi_0 = \sum_{\mathbf{w} \in \mathcal{L}_0} \Psi_{\mathbf{w}}. \quad (32)$$

where $\kappa(x) = x/(1+x)$. In the initial stage of the algorithm the amplitudes of the solution states are small and $|\Phi_0| \sim |\tilde{\Phi}| \sim 2^{-n}$. When these terms are neglected $\Phi \approx \bar{\Phi}$, and (30) gives a closed-form algebraic equation for λ which solution $\lambda_0^i(\tau) \approx \alpha(\tau)V_0 - 2\mu\tau + \mathcal{O}(\mu^2)$ accurately tracks the adiabatic ground state energy, from $\tau = 0$, up until the small vicinity of the avoided-crossing, $\tau \approx \tau^*$ (see below) where $|\Phi_0| \sim 1$. In this region (and also for $\tau > \tau^*$) one needs to retain the terms $\propto \Phi_0$ in Eq.(30) that couple it to the equations for $\tilde{u}_{\mathbf{z}}$ and $\Psi_{\mathbf{w}}$.

We express the components $\tilde{u}_{\mathbf{z}}$ in terms of the amplitudes $\Psi_{\mathbf{w}}$ by inverting the equation for $\tilde{u}_{\mathbf{z}}$ in (30) with sequential iterations. The result is substituted into the sum $\sum_{\mathbf{z} \notin \mathcal{L}_0} \mathcal{J}_{d(\mathbf{z}, \mathbf{w})} \tilde{u}_{\mathbf{z}}$ that enters equation for $\Psi_{\mathbf{w}}$ (cf. (23)). A key observation is that the dominant contribution to this sum comes from the states \mathbf{z} that are one bit-flip away from the states \mathbf{w} : $r = d(\mathbf{z}, \mathbf{w}) = 1$ (cf. Eq.(28)). This can be seen from the fact that amplitudes $\tilde{u}_{\mathbf{z}}$ corresponding to not very large $r \ll n$, are scaled with n as $n^{-(r+1)}$ and also from the form of \mathcal{J}_r above. The contribution to the sum from the rest of terms ($r > 1$) is $\mathcal{O}(n^{-2})$. Finally, after excluding $\tilde{u}_{\mathbf{z}}$ from the equations for $\Psi_{\mathbf{w}}$ in (23) and using (30),(32) we obtain a closed-form equation for λ . We give it below in the region of interest $|\tau - 1/2| \ll 1$

$$(\lambda - \lambda_0^i(\tau)) (\lambda - \lambda_0^f(\tau)) = -n^2 2^{-n} \Delta^2 / 4 \quad (33)$$

$$\Delta \approx d_0^{1/2} (1 + \mu\tau \ln 2 + \mathcal{O}(\mu^2)).$$

The form of $\lambda_0^i(\tau)$ is given above and $\lambda_0^f(\tau) \approx \tau \varepsilon_0 + 1/2$ is another branch of the eigenvalues that eventually approaches ε_0 for $\tau \rightarrow 1$.

The minimum gap between the two roots of (33) is $g_{\min} = n \Delta 2^{-n/2}$ and it is achieved at the point $\tau = \tau^*$ where the branches $\lambda_0^i(\tau)$, $\lambda_0^f(\tau)$ cross each other, $\tau^* \approx 1/2 + \log_2(d_0/\mu)/(4n)$. Based on the above analysis one can estimate the matrix element $H_{01}^* \sim n$ in (14). Then the complexity of the quantum adiabatic algorithm is, $d_0 H_{01}^*/g_{\min}^2 \sim (n d_0)^{-1} 2^n$. To logarithmic accuracy the results are in agreement with the numerical simulations results given above.

It follows from the discussion above that eigenvalue branch $\lambda_0^i(\tau)$ corresponds to an *extended* state $\sum_{\mathbf{z}} \tilde{u}_{\mathbf{z}} |\mathbf{z}\rangle$ with exponentially small individual amplitudes, $|\tilde{u}_{\mathbf{z}}| \sim 2^{-n/2}$ (cf. (30)). On the other hand $\lambda_0^f(\tau)$ corresponds to a localized state ($|\Phi_0|, |\tilde{\Phi}| \sim 1$) and therefore the coupling between the two states is exponentially small (cf. r.h.s. in Eqs. (30) and (33)). A similar picture applies to the avoided-crossing of the extended state energy $\lambda_0^i(\tau)$ with energies of localized states $\lambda_k^f(\tau)$ corresponding to $\mathbf{z} \in \mathcal{L}_k$ with $k \ll n$. The existence of the extended eigenstate of $\tilde{H}(\tau)$ at later times, $\tau \gtrsim \tau^*$, whose properties do not depend on a particular instance of SPP can be explained as follows. According to (18)-(23), matrix elements of the Green function associated with the driver Hamiltonian $\langle \mathbf{z}' | (\lambda - \alpha V)^{-1} | \mathbf{z} \rangle$ depend only on a Hamming distance $r = d(\mathbf{z}, \mathbf{z}')$; on the other hand it follows from the above that the joint distribution of energies $\rho_r(E, E')$ factorizes

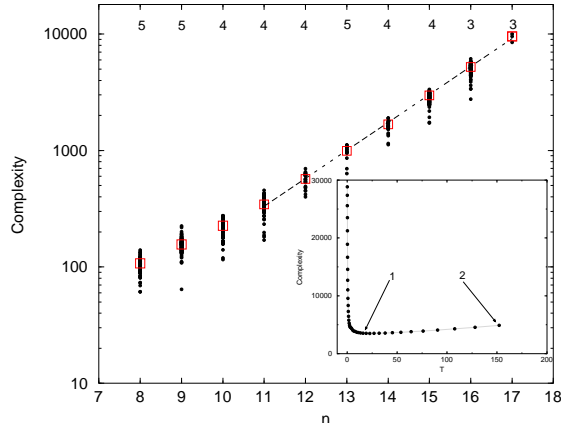


FIG. 1: Logarithmic plot of C_{\min} vs n for randomly generated instances of SPP with 25-bit precision numbers. Vertical sets of points indicate results of different trials (~ 100 trials for each n , except $n=17$). Median values of C_{\min} are shown with rectangles. Linear fit to the logarithmic plot of median values for n between 11 and 17 is shown by the line and gives $\ln C_{\min} \approx 0.55n$ ($C_{\min} \sim 2^{0.8n}$). Very close result is obtained for the linear fit if all data points are used instead of the median values. *Insert:* plot of $C(T)$ vs T for $n=15$, precision $b=25$ bits, $d_0=22$. Point 1 indicated with the arrow refers to the minimal value of complexity at $T = T_{\min} = 22.67$ where the total population of a ground level $p_0(T_{\min}) = 0.15$. Point 2 refers to the value of T where $p_0(T) = 0.7$.

for not too large energies (cf. [18]), and therefore the structure of the problem is being averaged out during the quantum evolution that begins from the symmetric state (12).

We also study the complexity of the algorithm by numerical integration of the time-dependent Schrödinger equation with Hamiltonian $H(t)$ and initial state $|\psi(0)\rangle$ defined in Eqs. (11),(12),(15)-(17). Here we relax the condition $\omega_M \ll \langle E \rangle$ used above in the analytical treatment of the problem; in simulations the value of M is set automatically to be an integer closest to $\log_2 \sum_{j=0}^n a_j$ (cf. (16)). We introduce a complexity metric for the algorithm, $C(T) = (1 + T)d_0/p_0(T)$ where $p_0(t) =$

$\sum_{\mathbf{w} \in \mathcal{L}_0} |\psi_{\mathbf{w}}(t)|^2$. A typical plot of $C(T)$ for an instance of the problem with $n=15$ numbers is shown in the insert of Fig. 1. At very small T the wavefunction is close to the symmetric initial state and the complexity is $\sim 2^n$. The extremely sharp decrease in $C(T)$ with T is due to the buildup of the population $p_0(T)$ in the ground level, $\mathcal{E}_{\mathbf{z}} = \varepsilon_0$, as quantum evolution approaches the adiabatic limit. At certain $T = T_{\min}$ the function $C(T)$ goes through the minimum: for $T > T_{\min}$ the decrease in the number of trials $d_0/p_0(T)$ does not compensate anymore for the overall increase in the runtime T for each trial. For a given problem instance the “minimal” complexity $C_{\min} = C(T_{\min})$ is obtained via one dimensional minimization over T . Plot of the complexity C_{\min} for different values of n in Fig. 1 appears to indicate the exponential scaling law, $C_{\min} \sim 2^{0.8n}$ for not too small values of $n \gtrsim 11$.

In conclusion, we have studied both analytically and numerically, the complexity of the quantum adiabatic algorithm applied to large random instances of SPP. We obtained the asymptotic behavior of the minimal gap that scales exponentially with problem size n . Analytical results for the algorithm’s complexity are in qualitative agreement with the results of numerical simulations of the algorithm for small-to-moderate values of n . We also developed a general technique for the analyzes of quantum spin-glass problems based on the separation of fast- and slow-varying parts of the wavefunction and the related picture of avoided crossing between the energies of extended and localized states (as the system parameters vary). This approach can be applied to different examples of random COPs where one searches for the solution using continuous-time quantum algorithms. Among the other applications is the analysis of tunneling phenomenon in the low-temperature dynamics of random magnets.

The authors benefited from stimulating discussions with D. A. Timucin, and R.D. Morris. This research was supported by NASA IS/RC program through Grant No:xxx, and also by the NASA Ames NAS facility.

-
- [1] P.W. Shor, in *Proceedings of the 35th Annual Symposium on the Foundations of Computer Science*, ed. by S. Goldwasser (IEEE Computer Society Press, Los Alamitos, CA, 1994), p.124.
 - [2] Y. Fu and P.W. Anderson, *J. Phys. A: Math. Gen.* **19**, 1605-1620 (1986).
 - [3] M. Mezard, G. Parisi, and M. Virasoro, *Spin glass theory and beyond* (World Scientific, Singapore, 1987).
 - [4] M.R. Garey and D.S. Johnson, *Computers and Intractability. A Guide to the Theory of NP-Completeness* (W.H. Freeman, New York, 1979).
 - [5] E. Farhi, J. Goldstone, S. Gutmann, and M. Sipser, arXiv:quant-ph/0001106.
 - [6] E. Farhi, J. Goldstone, S. Gutmann, J. Lapan, A. Lundgren, and D. Preda, *Science* **292**, 472 (2001).
 - [7] E. Farhi, J. Goldstone, and S. Gutmann, arXiv:quant-ph/0007071.
 - [8] A. M. Childs, E. Farhi, J. Goldstone, and S. Gutmann, arXiv:quant-ph/0012104.
 - [9] E. Farhi, J. Goldstone, S. Gutmann, arXiv:quant-ph/0201031.
 - [10] Li-Hui Tsai, *SIAM J. Comput.*, **21**(1) p.59-64 (1992).
 - [11] A. Shamir, *Proc. of 11th Annual ACM Symposium on Theory of Computing*, p.118 (1979).
 - [12] D.S. Johnson, et al., *Operations Research* **39**, p.378 (1991).
 - [13] F.F. Ferreira and J. F. Fontanari, *J. Phys. A* **31**, p. 3417 (1998).

- [14] I.P. Gent and T. Walsh, in Proc. of the ECAI-96, ed. by W. Wahlster (John-Wiley & Sons, New York, 1996), pp. 170-174.
- [15] R.E. Korf, Artificial Intelligence **106**, 181 (1998).
- [16] S. Mertens, Phys. Rev.Lett. **81**, 4281-4284 (1998).
- [17] Artif. Intel. **81** (1-2) (1996), special issue on Topic, ed. by T. Hogg, B.A. Huberman, and C. Williams.
- [18] S. Mertens, Phys. Rev.Lett. **84**, 1347-1350 (2000).
- [19] S. Lloyd, Science **273**, 1073 (1996).